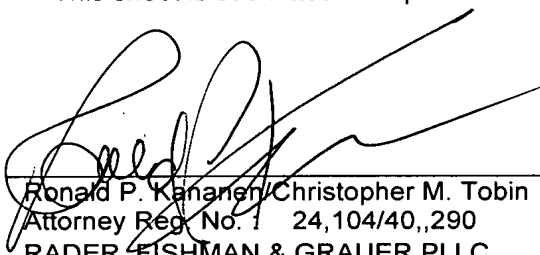| TRANSMITTAL OF APPEAL BRIEF	Docket No. SON-2320

In re Application of: Makoto Oka et al.

Application No. 10/041,964-Conf. #4260	Filing Date January 9, 2002	Examiner W. S. Powers	Group Art Unit 2134

Invention:	PUBLIC KEY CERTIFICATE ISSUING SYSTEM, PUBLIC KEY CERTIFICATE ISSUING METHOD, DIGITAL CERTIFICATION APPARATUS, AND PROGRAM STORAGE MEDIUM

TO THE COMMISSIONER OF PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed: May 14, 2007   .

The fee for filing this Appeal Brief is $ 500.00   .

[x] Large Entity   [ ] Small Entity

[ ] A petition for extension of time is also enclosed.

The fee for the extension of time is   _____   .

[ ] A check in the amount of   _____   is enclosed.

[x] Charge the amount of the fee to Deposit Account No.   18-0013   .
This sheet is submitted in duplicate.

[ ] Payment by credit card. Form PTO-2038 is attached.

[x] The Director is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No.   18-0013   .
This sheet is submitted in duplicate.

Dated: July 16, 2007

Ronald P. Kananen/Christopher M. Tobin
Attorney Reg. No.   24,104/40,,290
RADER, FISHMAN & GRAUER PLLC
1233 20th Street, N.W.
Suite 501
Washington, DC 20036
(202) 955-3750

Docket No.: SON-2320
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Makoto OKA et al.

Confirmation No.: 4260

Application No.: 10/041,964

Art Unit: 2134

Filed: January 9, 2002

Examiner: W. S. Powers

For: PUBLIC KEY CERTIFICATE ISSUING
SYSTEM, PUBLIC KEY CERTIFICATE
ISSUING METHOD, DIGITAL
CERTIFICATION APPARATUS, AND
PROGRAM STORAGE MEDIUM

APPELLANT'S BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This is an Appeal Brief under 37 C.F.R. §41.37 appealing the final decision of the Examiner dated February 7, 2007. Each of the topics required by 37 C.F.R. §41.37 is presented herewith and is labeled appropriately. This Brief is in furtherance of the Final Office Action on February 7, 2007.

A Notice of Appeal was filed in this case on May 14, 2007, along with a Request for Panel Review and a *one-month* extension.

The Notice of Panel Decision from Pre-Appeal Brief Review mailed on June 20, 2007 ("the Decision) indicates that claims 1-36 remain rejected.

The Decision further indicates that the extendable time period for the filing of the Appellant's Brief will be reset to be one month from the mailing of the Decision. Accordingly, the filing of the Brief is timely.

I.   REAL PARTY IN INTEREST

Sony Corporation of Tokyo, Japan ("Sony") is the real party in interest of the present application. An assignment of all rights in the present application to Sony was executed by the inventor and recorded by the U.S. Patent and Trademark Office at **reel 012786, frame 0401**.

II.   RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III.   STATUS OF CLAIMS

Within the Final Office Action of February 7, 2007:

Page 2 of the Final Office Action includes a rejection of claims 1-3, 5, 6, 9, 10, 12-17, 19, 20, 22-25, 27, 28, 31, 32, and 34-36 under 35 U.S.C. § 102(b) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al.

Page 3 of the Final Office Action includes a rejection of claims 4, 7, 26, and 29 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al. in view of U.S. Patent No. 6,202,157 to Brownlie et al.

Page 3 of the Final Office Action includes a rejection of claims 8, 18, and 30 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al. in view of "On the Importance of Checking Cryptographic Protocols for Faults" by Boneh et al.

Page 4 of the Final Office Action includes a rejection of claims 11, 21, and 33 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al. in view of U.S. Patent No. 6,675,296 to Boeyen et al.

Thus, the status of the claims is as follows:

Claims 1-36: (Rejected)

No claims are indicated within the Final Office Action to contain allowable subject matter.

Accordingly, Appellant hereby appeals the final rejection of claims 1-36 which are presented in the Claims Appendix.

IV.   STATUS OF AMENDMENTS

Subsequent to the final rejection of February 7, 2007, no amendment After Final Action has been entered.

V.   SUMMARY OF CLAIMED SUBJECT MATTER

The following description is provided for illustrative purposes and is not intended to limit the scope of the invention.

The present invention relates to a public key certificate issuing system including a certificate authority and a registration authority. The certificate authority issues public key certificates for use by entities. The registration authority operates as a proxy between the entities and the certificate authority. When a registration authority receives a public key certificate issuance request from an entity under its jurisdiction, the registration authority transmits the received request to the certificate authority. The certificate authority includes a plurality of signature modules each executing a different signature algorithm. When the certificate authority receives a request from an entity, through the registration authority, the certificate authority selects at least one of the plurality of signature modules in accordance with the registration authority passing the request, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate.

Claims 1-4 and 8-13 stand or fall together: - Claims 2-13 are dependent upon claim 1. Claim 1 is drawn to a public key certificate issuing system comprising:

a certificate authority (70, 100, 321, 401) for issuing a public key certificate (fig. 1, figs 21-24, element 9) used by an entity (300, Specification ¶0099, end entities EE); and

a registration authority (81-85, 181-183, 311-312, 402) which, on receiving a public key certificate issuance request (figs 21-24, element 3) from any one of entities (300, Specification ¶0099, "end entities EE") under jurisdiction thereof, transmits the received request (figs 21-24, element 1) to said certificate authority (70, 100, 321, 401);

wherein said certificate authority, having a plurality of signature modules (72a-n, 150a-c, 331-332) each executing a different encryption algorithm, selects at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority (81-85, 181-183, 311-312, 402) based upon an identification of an assigned encryption algorithm, said identification of the assigned algorithm being made with reference to a table (fig. 11, 21, RA Management Database) that associates the registration authority with the assigned encryption algorithm (figs. 11, 21, "RAID" and "HSM In Use"), and causes the selected signature module to attach a digital signature to message data constituting a public key certificate (fig 1, "Digital Signature").

Claims 5 stands or falls alone: Claim 5 is drawn to a public key certificate issuing system as recited in claim 3, wherein said registration authority management data (fig. 25, element 402, "structure management table") include signature module identification information applicable to signatures.

Claims 6 and 7 stands or fall together: Claim 7 is dependent upon claim 6. Claim 6 is drawn to a public key certificate issuing system according to claim 1, wherein said registration authority (81-85, 181-183, 311-312, 402) transmits encryption algorithm designation information along with said public key certificate issuance request to said certificate authority (70, 100, 321, 401); and

wherein said certificate authority, based on said encryption algorithm designation information (fig. 24, (a) certificate issuance request "signature algorithm") received along with said public key certificate issuance request, selects a signature module applicable to the designated encryption algorithm(figs. 11, 21, "RAID" and "HSM In Use").

Claims 14-15 and 17-22 stand or fall together: - Claims 15-22 are dependent upon claim 14. Claim 14 is drawn to a public key certificate issuing method for use with a certificate authority (70, 100, 321, 401) for issuing a public key certificate (fig. 1, figs 21-24, element 9) used by an entity (300, Specification ¶0099, end entities EE), and with a registration authority (81-85, 181-183, 311-312) which, on receiving a public key certificate issuance request (figs 21-24, element 3) from any one of the entities (300, Specification ¶0099, "end entities EE") under jurisdiction thereof, transmits the received request (figs 21-24, element 1) to said certificate authority (70, 100, 321, 401), the method comprising the steps of:

> causing said certificate authority to select (S232) from among a plurality of signature modules (72a-n, 150a-c, 331-332) each executing a different encryption algorithm , at least one of the signature modules (S232) in accordance with said public key certificate issuance request (S251) from said registration authority based upon an identification of an assigned encryption algorithm for the registration authority(81-85, 181-183, 311-312), said identification of the assigned algorithm being made with reference to a table (fig. 11, 21, RA Management Database) that associates the registration authority with the assigned encryption algorithm (figs. 11, 21, "RA ID" and "HSM In Use"); and

> causing the selected signature module to attach a digital signature to message data constituting a public key certificate (fig. 1, "Digital Signature").

Claims 16 stands or falls alone: Claim 16 is drawn to a public key certificate issuing method according to claim 15, wherein said step involving said certificate authority server (70, 100, 321, 401) selecting (S232) the signature module comprises selecting (S252) the signature module based on a registration authority management database (fig. 11, 21, RA Management Database) which stores registration authority management data for associating registration authorities issuing public key certificate issuance requests with an encryption algorithm specific to each of said registration authorities (81-85, 181-183, 311-312, 402).

Claims 23-26 and 30-35 stand or fall together: - Claims 24-35 are dependent upon claim 23. Claim 23 is drawn to a digital certification apparatus for constituting a certificate authority (70, 100, 321, 401) which issues a public key certificate (fig. 1, figs 21-24, element 9)

used by an entity in association with a request transmitted to the certificate authority by a registration authority (81-85, 181-183, 311-312, 402):

> wherein said digital certification apparatus, having a plurality of signature modules (72a-n, 150a-c, 331-332) each executing a different encryption algorithm, selects (S232, fig 20) at least one of said plurality of signature modules in accordance with a public key certificate issuance request (S251) received from outside said digital certification apparatus and based upon an identification of an assigned encryption algorithm for the registration authority, said identification of the assigned algorithm being made with reference to a table (figs. 11, 21, "RA Management Database") that associates the registration authority with the assigned encryption algorithm, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate (fig 1, "Digital Signature").

Claims 27 stands or falls alone: Claim 25 is drawn to a digital certification apparatus as recited in claim 25, wherein said registration authority management data (fig. 25, element 402, "structure management table") include signature module identification information applicable to signatures.

Claims 28 and 29 stand or fall together: Claim 29 is dependent upon claim 28. Claim 28 is drawn to a digital certification apparatus according to claim 23, wherein said digital certification apparatus, based on encryption algorithm designation information (fig. 25, element 402, "structure management table") received along with said public key certificate issuance request, selects a signature module applicable to the designated encryption algorithm.

Claims 36 stands or falls alone: Claim 36 is drawn to a program storage medium which stores a computer program executed by a computer system in carrying out public key certificate issuance processing to issue a public key certificate (fig 1, "Digital Signature") for use by an entity (300, Specification ¶0099, "end entities EE"), said computer program comprising the steps of:

> selecting, from among a plurality of signature modules (72a-n, 150a-c, 331-332) each executing a different encryption algorithm, at least one of the signature modules

in accordance with a public key certificate issuance request (S251) and with reference to a table (figs. 11, 21, "RA Management Database") that associates the registration authority (81-85, 181-183, 311-312, 402) with an assigned encryption algorithm; and

causing the selected signature module to attach a digital signature to message data constituting a public key certificate (S241-S243).

VI.   GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The issues presented for consideration in this appeal are as follows:

Whether the Examiner erred in rejecting claims 1-3, 5, 6, 9, 10, 12-17, 19, 20, 22-25, 27, 28, 31, 32, and 34-36 under 35 U.S.C. § 102(b) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al.

Whether the Examiner erred in rejecting claims 4, 7, 26, and 29 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth in view of U.S. Patent No. 6,202,157 to Brownlie et al.

Whether the Examiner erred in rejecting claims 8, 18, and 30 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth in view of "On the Importance of Checking Cryptographic Protocols for Faults" by Boneh et al.

Whether the Examiner erred in rejecting claims 11, 21, and 33 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth in view of U.S. Patent No. 6,675,296 to Boeyen et al.

These issues will be discussed herein below.

VII.   ARGUMENT

In the Office Action of February 7, 2007:

The Final Office Action erroneously rejects claims 1-3, 5, 6, 9, 10, 12-17, 19, 20, 22-25, 27, 28, 31, 32, and 34-36 under 35 U.S.C. § 102(b) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al.

The Final Office Action erroneously rejects claims 4, 7, 26, and 29 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al. in view of U.S. Patent No. 6,202,157 to Brownlie et al.

The Final Office Action erroneously rejects claims 8, 18, and 30 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al. in view of "On the Importance of Checking Cryptographic Protocols for Faults" by Boneh et al.

The Final Office Action erroneously rejects claims 11, 21, and 33 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al. in view of U.S. Patent No. 6,675,296 to Boeyen et al.

For at least the following reasons, Appellant submits that these rejections are both technically and legally unsound and should therefore be reversed.

For purposes of this appeal brief only, and without conceding the teachings of any prior art reference, the claims have been grouped as indicated below.

The Final Office Action erroneously rejects claims 1-3, 5, 6, 9, 10, 12-17, 19, 20, 22-25, 27, 28, 31, 32, and 34-36 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,035,402 to Vaeth et al. ("Vaeth").

These rejections are traversed at least for the following reasons.

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California,* 814 F.2d 628, 631 (Fed. Cir. 1987).

Claims 1-4 and 8-13 stand or fall together: - Vaeth arguably discloses a Virtual Certificate Authority where requests for a certificate and verification information are directed to

the Certificate Authority (CA) from a plurality of entities, directly or through a Registration Authority (RA).

Vaeth discloses a three-entity relationship used to produce certificates. At the top-tier of the hierarchy is the Certification Authority (CA). At the bottom-tier are the Entities (Vaeth, fig. 3: elements 170, 178, 179) which issue requests for certificates. An Entity will issue a request for a certificate through a Registration Authority (RA) (Vaeth, fig. 3: elements 180) or directly to the Certification Authority (CA) (Vaeth, fig. 3: elements 190). The RA is positioned in the middle-tier, in one of two capacities. In a first capacity the RA will retrieve requests from the CA and verify the entities makings the requests (Vaeth at 7:48-51). In a second capacity the RA will receive certificate request from an Entity and relay the request to the CA, once the Entity is verified (Vaeth at 7:58-63).

The CA implements generic or specialized cryptography functions using a combination of crypto-cards to produce different types of certificates (Vaeth, fig. 3: elements 246-249, and at 7:36-40). The CA executes a particular combination of generic or specialized certificate functions, based on the requesting Entity, to produce a certificate. The combination of generic or specialized certificate functions executed by the CA is directly dependent on the requesting Entity.

The CA produces each type of certificate based on the association between certificate types and requesting entities.

There is no disclosed certificate related relationship between the RA used to make a given certificate request and the type of certificates the CA issues. The type of certificate issued by the CA is only based on the requesting Entity. This allows a given entity to make a requests for the same type certificate through multiple RAs, and for the implementation of schemes wherein a single entity can obtain similar types of certificates through one of multiple RAs. (Vaeth, fig. 3: elements 180 and 188, and at 8:52-59).

In Vaeth, a CA may be configured to provide specialized functions for each entity, such as for cardholders, merchants, and payment gateways (Vaeth at 7:30-35). To do this, the CA uses a variety of crypto-cards that respectively perform cryptographic functions, including the

generation of the particular type of certificate. However, the CA only executes the crypto-cards associated *with a given entity to produce a given certificate.* (Vaeth at 7:34-47).

There is no mention or suggestion that the applicable crypto-card is based on the RA associated with a given requesting entity. These different cryptographic functions, provided by the crypto-cards of Vaeth, are apparently directed at the general differences that are required for the *different roles of the entities.* For example, the functions provided by the CA may be different for a cardholder as opposed to a merchant.

Within claim 1, the certification authority identifies which signature modules (72a-n, 150a-c, 331-332) to execute in order to produce public key certificate, based on a table (fig. 11, 21, RA Management Database) that associates the registration authority with the assigned encryption algorithm (fig. 11, 21, "RAID" and "HSM In Use"). However, since Vaeth does not associate public key certificates with particular RA's, Vaeth does not teach or suggest "a table that associates the registration authority with the assigned encryption algorithm."

As discussed above, in the three-tier hierarchy disclosed in independent claim 1, the type of certificate produced by the Certification Authority (CA) is based on the Registration Authority (RA), **which resides in the middle-tier**.

Conversely, in Vaeth the combination of encryption algorithms executed by the Certification Authority (CA) to produce a public key certificate is based on the Entity making that request, **which resides in the bottom-tier**.

Accordingly, Vaeth <u>fails</u> to teach or suggest that the type of certificate produced by the Certification Authority (CA) is based on the requesting Registration Authority (RA).

- *Thus, Vaeth <u>fails</u> to disclose, teach or suggest wherein said certificate authority, having a plurality of signature modules each executing a different encryption algorithm, selects at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority based upon an identification of an assigned encryption algorithm, said identification of the assigned algorithm being made with reference to <u>a table that associates the</u>*

registration authority with the assigned encryption algorithm, and causes the
selected signature module to attach a digital signature to message data constituting a
public key certificate.

Claims 5 stands or falls alone: In Vaeth, the Certification Authority (CA) produces the
type of certificates based on the requesting entities, not based on signature module information
from the RA.

Page 5 of the Final Office Action cites to Vaeth at 7:41-47 and 8:49-9:12, as a basis that
Vaeth discloses that the RA management data includes signature module information applicable
to the signatures.

However, at 7:41-47. Vaeth only discloses that the CA uses multiple crypto-cards, and at
8:49-9:12 Vaeth clearly teaches that multiple entities can use the same RA to request different
types of certificates from the Certification Authority (CA) produces the type of certificates based
on the requesting entities (Vaeth at 9:5-9). In the same paragraph, Vaeth discloses that a given
entity can make requests through different RAs, particularly because the type of certificate does
not depend of the requesting RA (Vaeth at 9:8-12). However, nowhere does Vaeth disclose that
the type of certificate issued by the CA is based on the RA authenticating a given entity.

- *Thus, Vaeth fails to disclose, teach or suggest wherein said registration authority*
  management data include signature module identification information applicable to
  signatures.

Claims 6 and 7 stand or fall together: Vaeth does not disclose using information from
the RA to determine which encryption algorithm to use to produce given type of certificate.

Page 7 of the Final Office Action cites to Vaeth at 7:41-47 and 8:49-9:12, as a basis that
Vaeth discloses that the RA transmits encryption algorithm designation information along with
said public key certificate issuance request.

However, as disclosed above, Vaeth does not disclose employing information from an
RA to decide which crypto-card to use to produce a given certificate. While Vaeth uses the RA

to decide whether an entity is *authorized* to make a request, Vaeth does not indicate that the *authorization* includes *encryption algorithm designation information.*

- *Thus, Vaeth fails to disclose, teach or suggest wherein said registration authority transmits encryption algorithm designation information along with said public key certificate issuance request to said certificate authority.*

Claims 14-15 and 17-22 stand or fall together: - Vaeth fails to teach or suggest that the type of certificate produced by the Certification Authority (CA) is based on a Registration Authority (RA).

- *Thus, Vaeth fails to disclose, teach or suggest causing said certificate authority to select from among a plurality of signature modules each executing a different encryption algorithm , at least one of the signature modules in accordance with said public key certificate issuance request from said registration authority based upon an identification of an assigned encryption algorithm for the registration authority, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with the assigned encryption algorithm.*

Claims 16 stands or falls alone: In Vaeth, the Certification Authority (CA) produces the type of certificates based on the requesting entities, not based on signature module information from the RA.

- *Thus, Vaeth fails to disclose, teach or suggest, wherein said step involving said certificate authority server selecting the signature module comprises selecting the signature module based on a registration authority management database which stores registration authority management data for associating registration authorities issuing public key certificate issuance requests with a encryption algorithm specific to each of said registration authorities.*

Claims 23-26 and 30-35 stand or fall together: - Vaeth fails to teach or suggest that the type of certificate produced by the Certification Authority (CA) is based on a Registration Authority (RA).

- *Thus, Vaeth fails to disclose, teach or suggest wherein said digital certification apparatus, having a plurality of signature modules each executing a different encryption algorithm, selects at least one of said plurality of signature modules in accordance with a public key certificate issuance request received from outside said digital certification apparatus and based upon an identification of an assigned encryption algorithm for the registration authority, said identification of the assigned algorithm being made with reference to <u>a table that associates the registration authority with the assigned encryption algorithm</u>, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate.*

Claims 27 stands or falls alone: In Vaeth, the Certification Authority (CA) produces the type of certificates based on the requesting entities, not based on signature module information from the RA.

- *Thus, Vaeth fails to disclose, teach or suggest wherein said registration authority management data include signature module identification information applicable to signatures.*

Claims 28 and 29 stand or fall together: Vaeth does not disclose using information from the RA to determine which encryption algorithm to use to produce given type of certificate.

- *Thus, Vaeth fails to disclose, teach or suggest wherein said digital certification apparatus, based on encryption algorithm designation information received along with said public key certificate issuance request, selects a signature module applicable to the designated encryption algorithm.*

Claims 36 stands or falls alone: - Vaeth <u>fails</u> to teach or suggest that the type of certificate produced by the Certification Authority (CA) is based on the requesting Registration Authority (RA).

- *Thus, Vaeth <u>fails</u> to disclose, teach or suggest selecting, from among a plurality of signature modules each executing a different encryption algorithm, at least one of the*

signature modules in accordance with a public key certificate issuance request and with reference to a table that associates the registration authority with an assigned encryption algorithm.

The Final Office Action erroneously rejects claims 4, 7, 26, and 29 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al. (Vaeth) in view of U.S. Patent No. 6,202,157 to Brownlie et al. (Brownlie).

Brownlie discloses a network security system capable of applying security policy provisions issued at a centralized authority to various network nodes, which in turn verify the policy provisions using digital signatures associated with the central authority.

However, Brownlie fails to teach or suggest a certification scheme that associates the registration authority with an assigned encryption algorithm.

Thus, Brownlie fails to disclose, teach, or suggest that *said identification of the assigned algorithm [is] made with reference to a table that associates the registration authority with the assigned encryption algorithm.*

The Final Office Action erroneously rejects claims 8, 18, and 30 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al. (Vaeth) in view of "On the Importance of Checking Cryptographic Protocols for Faults" by Boneh et al. (Boneh).

Boneh describes how various authentication protocols can be broken using hardware faults.

However, Brownlie fails to teach or suggest the distribution of encrypted certificates.

- *Thus, Boneh fails to disclose, teach, or suggest that said identification of the assigned algorithm [is] made with reference to a table that associates the registration authority with the assigned encryption algorithm.*

__The Final Office Action erroneously rejects claims 11, 21, and 33 under 35 U.S.C. § 103(a) as__
__being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al. (Vaeth) in view of__
__U.S. Patent No. 6,675,296 to Boeyen et al. (Boeyen).__

Boeyen discloses a certificate issuing apparatus and method to facilitate converting certificates between different formats. The Boeyen apparatus employs a series of templates representing different certificate formats, and maps the relevant data between the different formats.

However, Brownlie fails to teach or suggest a certification scheme or associating a registration authority with an encryption algorithm

- *Thus, Boeyen fails to disclose, teach, or suggest that said identification of the assigned algorithm [is] made with reference to a table that associates the registration authority with the assigned encryption algorithm.*

VIII. CLAIMS

A copy of the claims involved in the present appeal is attached hereto as Appendix A.

IX.   EVIDENCE

No evidence pursuant to §§ 1.130, 1.131, or 1.132, or additional evidence entered by or relied upon by the Examiner is being submitted.

X.   RELATED PROCEEDINGS

No related proceedings are referenced in section II above, or copies of decisions in related proceedings are not provided, hence no Appendix is included.

Conclusion

The claims are considered allowable for the reasons discussed above, as well as for the additional features they recite.

Reversal of the Examiner's decision is respectfully requested.

If any fee is required or any overpayment made, the Commissioner is hereby authorized to charge the fee or credit the overpayment to Deposit Account # 18-0013.

Dated: July 16, 2007

Respectfully submitted,

By_____
Ronald P. Kananen
    Registration No.: 24,104
Christopher M. Tobin
    Registration No.: 40,290
RADER, FISHMAN & GRAUER PLLC
Correspondence Customer Number: 23353
(202) 955-3750
Attorneys for Appellant

APPENDIX A: CLAIMS APPENDIX

<u>LISTING OF THE CLAIMS</u>

1. (Previously Presented) A public key certificate issuing system comprising:

a certificate authority for issuing a public key certificate used by an entity; and

a registration authority which, on receiving a public key certificate issuance request from any one of entities under jurisdiction thereof, transmits the received request to said certificate authority;

wherein said certificate authority, having a plurality of signature modules each executing a different encryption algorithm, selects at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority based upon an identification of an assigned encryption algorithm, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with the assigned encryption algorithm, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate.

2. (Previously Presented) A public key certificate issuing system according to claim 1, wherein said certificate authority has a certificate authority server for outputting a signature processing request to said plurality of signature modules;

wherein said certificate authority server receives said public key certificate issuance request from said registration authority, selects at least one of said plurality of signature modules in response to said public key certificate issuance request, and outputs said signature processing request to the selected signature module; and

wherein each selected signature module attaches a digital signature to the message data constituting said public key certificate in response to said signature processing request received from said certificate authority server.

3. (Previously Presented) A public key certificate issuing system according to claim 1, wherein said certificate authority has a registration authority management database which stores registration authority management data for associating registration authorities issuing public key certificate issuance requests with a encryption algorithm specific to each of said registration authorities; and

wherein, given a public key certificate issuance request from any registration authority, said certificate authority selects the signature module associated with the relevant encryption algorithm based on said registration authority management data.

4. (Previously Presented) A public key certificate issuing system according to claim 3, wherein said registration authority management data include key length and parameter information applicable to signatures.

5. (Previously Presented) A public key certificate issuing system according to claim 3, wherein said registration authority management data include signature module identification information applicable to signatures.

6. (Previously Presented) A public key certificate issuing system according to claim 1, wherein said registration authority transmits encryption algorithm designation information along with said public key certificate issuance request to said certificate authority; and

wherein said certificate authority, based on said encryption algorithm designation

information received along with said public key certificate issuance request, selects a signature

module applicable to the designated encryption algorithm.

7. (Previously Presented) A public key certificate issuing system according to claim 6,

wherein said encryption algorithm designation information includes key length and parameter

information applicable to signatures.

8. (Previously Presented) A public key certificate issuing system according to claim 1,

wherein said certificate authority has a verification key database which stores keys for signature

verification in association with each of said plurality of signature modules; and

wherein said certificate authority verifies signatures generated by each of said plurality of

signature modules.

9. (Previously Presented) A public key certificate issuing system according to claim 1,

wherein said certificate authority uses at least two of said plurality of signature modules to attach

at least two different digital signatures to one public key certificate.

10. (Previously Presented) A public key certificate issuing system according to claim 1,

wherein said certificate authority selects at least two of said plurality of signature modules in

order to have signature processing executed in steps by each of the selected signature modules

used in concert for digital signature generation.

11. (Previously Presented) A public key certificate issuing system according to claim 1, wherein said certificate authority and said registration authority each have a signature module structure management table which associates encryption algorithm identifiers with identifiers of said plurality of signature modules;

wherein said registration authority issues to said certificate authority a public key certificate issuance request designating a encryption algorithm identifier in accordance with said signature module structure management table; and

wherein said certificate authority, upon receipt of said encryption algorithm identifier from said registration authority, selects the signature module applicable to the received identifier from said signature module structure management table.

12. (Previously Presented) A public key certificate issuing system according to claim 1, wherein at least part of said plurality of signature modules have a common signature key stored therein.

13. (Previously Presented) A public key certificate issuing system according to claim 1, wherein each of said plurality of signature modules is configured to execute multiple encryption algorithms.

14. (Previously Presented) A public key certificate issuing method for use with a certificate authority for issuing a public key certificate used by an entity, and with a registration authority which, on receiving a public key certificate issuance request from any one of entities under jurisdiction thereof, transmits the received request to said certificate authority, the method comprising the steps of:

causing said certificate authority to select, from among a plurality of signature modules

each executing a different encryption algorithm, at least one of the signature modules in

accordance with said public key certificate issuance request from said registration authority

based upon an identification of an assigned encryption algorithm for the registration authority,

said identification of the assigned algorithm being made with reference to a table that associates

the registration authority with the assigned encryption algorithm; and

causing the selected signature module to attach a digital signature to message data

constituting a public key certificate.

15. (Previously Presented) A public key certificate issuing method according to claim 14,

further comprising the steps of:

causing a certificate authority server to receive a public key certificate issuance request

from said registration authority;

causing said certificate authority server to select at least one of said plurality of signature

modules in response to said public key certificate issuance request; and

causing said certificate authority server to output a signature processing request to the

selected signature module.

16. (Previously Presented) A public key certificate issuing method according to claim 15,

wherein said step involving said certificate authority server selecting the signature module

comprises selecting the signature module based on a registration authority management database

which stores registration authority management data for associating registration authorities

issuing public key certificate issuance requests with a encryption algorithm specific to each of

said registration authorities.

17. (Previously Presented) A public key certificate issuing method according to claim 15, wherein said step involving said certificate authority server selecting the signature module comprises selecting the signature module based on encryption algorithm designation information received along with said public key certificate issuance request.

18. (Previously Presented) A public key certificate issuing method according to claim 14, further comprising the step of causing said certificate authority to verify signatures generated by each of said plurality of signature modules.

19. (Previously Presented) A public key certificate issuing method according to claim 14, further comprising the step of causing said certificate authority to use at least two of said plurality of signature modules to attach at least two different digital signatures to one public key certificate.

20. (Previously Presented) A public key certificate issuing method according to claim 14, further comprising the step of causing said certificate authority to select at least two of said plurality of signature modules in order to have signature processing executed in steps by each of the selected signature modules used in concert for digital signature generation.

21. (Previously Presented) A public key certificate issuing method according to claim 14, wherein said certificate authority and said registration authority each have a signature module structure management table which associates encryption algorithm identifiers with identifiers of

said plurality of signature modules, said public key certificate issuing method further comprising the steps of:

causing said registration authority to issue to said certificate authority a public key certificate issuance request designating a encryption algorithm identifier in accordance with said signature module structure management table; and

causing said certificate authority, upon receipt of said encryption algorithm identifier from said registration authority, to select the signature module applicable to the received identifier from said signature module structure management table.

22. (Previously Presented) A public key certificate issuing method according to claim 14, wherein each of said plurality of signature modules is configured to execute multiple encryption algorithms.

23. (Previously Presented) A digital certification apparatus for constituting a certificate authority which issues a public key certificate used by an entity in association with a request transmitted to the certificate authority by a registration authority:

wherein said digital certification apparatus, having a plurality of signature modules each executing a different encryption algorithm, selects at least one of said plurality of signature modules in accordance with a public key certificate issuance request received from outside said digital certification apparatus and based upon an identification of an assigned encryption algorithm for the registration authority, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with the assigned encryption algorithm, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate.

24. (Previously Presented) A digital certification apparatus according to claim 23, further comprising a plurality of signature modules and a certificate authority server for outputting a signature processing request to said plurality of signature modules;

wherein said certification authority server receives said public key certificate issuance request, selects at least one of said plurality of signature modules in response to said public key certificate issuance request, and outputs said signature processing request to the selected signature module; and

wherein each selected signature module attaches a digital signature to the message data constituting said public key certificate in response to said signature processing request received from said certificate authority server.

25. (Previously Presented) A digital certification apparatus according to claim 23, further comprising a registration authority management database which stores registration authority management data for associating registration authorities issuing public key certificate issuance requests with a encryption algorithm specific to each of said registration authorities;

wherein, given a public key certificate issuance request from any registration authority, said digital certification apparatus selects the signature module associated with the relevant encryption algorithm based on said registration authority management data.

26. (Previously Presented) A digital certification apparatus according to claim 25, wherein said registration authority management data include key length and parameter information applicable to signatures.

27. (Previously Presented) A digital certification apparatus according to claim 25, wherein said registration authority management data include signature module identification information applicable to signatures.

28. (Previously Presented) A digital certification apparatus according to claim 23, wherein said digital certification apparatus, based on encryption algorithm designation information received along with said public key certificate issuance request, selects a signature module applicable to the designated encryption algorithm.

29. (Previously Presented) A digital certification apparatus according to claim 28, wherein said encryption algorithm designation information includes key length and parameter information applicable to signatures.

30. (Previously Presented) A digital certification apparatus according to claim 23, further comprising a verification key database which stores keys for signature verification in association with each of said plurality of signature modules;

wherein said digital certification apparatus verifies signatures generated by each of said plurality of signature modules.

31. (Previously Presented)A digital certification apparatus according to claim 23, wherein said digital certification apparatus uses at least two of said plurality of signature modules to attach at least two different digital signatures to one public key certificate.

32. (Previously Presented) A digital certification apparatus according to claim 23, wherein said digital certification apparatus selects at least two of said plurality of signature modules in order to have signature processing executed in steps by each of the selected signature modules used in concert for digital signature generation.

33. (Previously Presented) A digital certification apparatus according to claim 23, further comprising a signature module structure management table which associates encryption algorithm identifiers with identifiers of said plurality of signature modules;

wherein said digital certification apparatus, upon receipt of a encryption algorithm identifier along with said public key certificate issuance request, selects the signature module applicable to the received identifier from said signature module structure management table.

34. (Previously Presented) A digital certification apparatus according to claim 23, wherein at least part of said plurality of signature modules have a common signature key stored therein.

35. (Previously Presented) A digital certification apparatus according to claim 23, wherein each of said plurality of signature modules is configured to execute multiple encryption algorithms.

36. (Previously Presented) A program storage medium which stores a computer program executed by a computer system in carrying out public key certificate issuance processing to issue a public key certificate for use by an entity, said computer program comprising the steps of:

selecting, from among a plurality of signature modules each executing a different encryption algorithm, at least one of the signature modules in accordance with a public key

certificate issuance request and with reference to a table that associates the registration authority

with an assigned encryption algorithm; and

    causing the selected signature module to attach a digital signature to message data

constituting a public key certificate.

APPENDIX B: EVIDENCE APPENDIX

There is no other evidence which will directly affect or have a bearing on the Board's decision in this appeal.

APPENDIX C: RELATED PROCEEDINGS APPENDIX

There are no other appeals or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.